ISAKMP Policy Configuration

This chapter describes how to create and verify ISAKMP (Internet Security Association Key Management Protocol) policies. ISAKMP is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment.

ISAKMP defines the procedures for authenticating a communicating peer, creation and management of Security Associations, key generation techniques and threat mitigation (for example, denial of service and replay attacks).

ISAKMP defines procedures and packet formats to establish, negotiate, modify and delete Security Associations. SAs contain all the information required for execution of various network security services, such as the IP layer services (header authentication and payload encapsulation), transport or application layer services or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

The following topics are discussed:

Process Overview

The basic sequence of actions required to configure an ISAKMP is outlined below.

Step 1 Configure a policy by applying the example configuration in Configuring ISAKMP Policy, on page 2.

Step 2 Verify your ISAKMP policy configuration by following the steps in Verifying the ISAKMP Policy Configuration, on page 2.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring ISAKMP Policy

Use the following example to create the ISAKMP policy on your system:

```
configure
   context ctxt_name
      ikev1 policy priority
         encryption { 3des-cbc | des-cbc }
         hash { md5 | sha1 }
         group { 1 | 2 | 3 | 4 | 5 }
         lifetime time
         end
```

Notes:

- *ctxt_name* is the system context in which you wish to create and configure the ISAKMP policy.
- *priority* dictates the order in which the ISAKMP policies are proposed when negotiating IKE SAs.
- For more information on parameters, refer to the *ISAKMP Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

Verifying the ISAKMP Policy Configuration

Enter the following Exec mode command for the appropriate context to display and verify your ISAKMP policy configuration:

show crypto isakmp policy *priority*

This command produces an output similar to that displayed below using the configuration of a transform set named test1.

```
1 ISAKMP Policies are configured
             Priority : 1
Authentication Method : preshared-key
             Lifetime : 120 seconds
            IKE group : 5
                 hash : md5
           encryption : 3des-cbc
```

Caution Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the **clear crypto security-association** command located in the *Exec Mode Commands* chapter of the *Command Line Interface Reference* for more information.